

Sidel'nikov 수열의 자기상관 분포

준회원 김 영 식*, 정 정 수*, 종신회원 노 종 선*, 정 하 봉**, 정회원 김 경 아***

On the Autocorrelation Distributions of Sidel'nikov Sequences

Young-Sik Kim*, Jung-Soo Chung* *Associate Member*,
Jong-Seon No*, Habong Chung** *Lifelong Member*, Kyung-ah Kim***, *Reguler Member*

요 약

이 논문에서는 Sidel'nikov 수열의 자기상관 분포, 다시 말해 자기상관 함수 각각의 값들의 발생 회수를 유도하였다. M -진 Sidel'nikov 수열의 각각의 상관 값들의 발생 회수는 M 차의 원분수를 이용해서 표현된다. 또한 서로 다른 자기 상관 값들의 총 개수는 알파벳 크기 M 뿐만 아니라 수열의 주기에도 의존하지만 언제나 $\binom{M}{2} + 1$ 보다 작거나 같다는 사실을 보였다.

Key Words : Autocorrelation, autocorrelation distribution, cyclotomic numbers, M -ary sequences, Sidel'nikov sequences.

ABSTRACT

In this paper, we derived the autocorrelation distributions, i.e., the values and the number of occurrences of each value of the autocorrelation function of Sidel'nikov sequences. The frequency of each autocorrelation value of an M -ary Sidel'nikov sequence is expressed in terms of the cyclotomic numbers of order M . It is also pointed out that the total number of distinct autocorrelation values is dependent not only on M but also on the period of the sequence, but always less than or equal to $\binom{M}{2} + 1$.

I. 서 론

전송 표준으로 M -진의 변조 방식을 사용하는 고속 데이터 통신의 수요가 증가하면서 좋은 오류 정정 능력을 갖는 M -진 부호와 좋은 상관 특성을 갖는 M -진 수열을 찾는 것이 더 중요해 지고 있다.

p 를 홀수의 소수라 할 때 $p-1$ 를 나누는 양의 정수 M 에 대해서(이것을 $M|(p-1)$ 로 나타낸다) Sidel'nikov는 자기상관특성 값들이 $\sqrt{5}$ 또는 3보다 작거나 같은 주기가 p 인 M -진 power residue 수열을 제안하였다 [1]. 그는 또한 $M|(p^n-1)$ 인 양의

정수 n 에 대해서 주기가 p^n-1 인 M -진 수열을 만들었다. 이 수열의 자기상관 값의 크기는 4보다 작거나 같다.

후에 Lempel, Cohn, 그리고 Eastman은 Sidel'nikov의 연구를 알지 못한 채로 주기가 p^n-1 인 이진 Sidel'nikove 수열을 다시 발견하였다 [2]. 이들 이진 수열들은 균형성을 고려했을 때 최적인 자기상관 특성을 가지고 있었다.

이 논문에서는 Sidel'nikov 수열의 자기상관 분포, 다시 말해 자기상관 함수의 각각의 값들의 발생 회수를 유도하였다. M -진 Sidel'nikov 수열의 각각의

* 서울대학교 전기컴퓨터공학부 부호 및 암호 연구실(jsno@snu.ac.kr)
** 홍익대학교 전자전기공학부, *** KT 통신망운용 연구소, 마케팅 연구소
논문번호 : KICS2005-06-045, 접수번호 : 2005년 6월 16일
※ 본 연구는 KT TETRA 과제의 연구결과로 수행되었음.

상관 값들의 발생 회수는 M 차의 원분수를 이용해서 표현된다. 또한 서로 다른 자기 상관 값들의 총 개수는 알파벳 크기 M 뿐만 아니라 수열의 주기에 의존하지만 언제나 $\binom{M}{2} + 1$ 보다 작거나 같다는 사실을 보였다.

II. 사전지식

$s(t)$ $0 \leq t \leq N-1$, 가 주기가 N 인 M -진 수열이고 ω_M 이 1의 M 차 복소근인 $\omega_M = e^{j2\pi/M}$ 라 하자. $s(t)$ 의 자기상관 함수는 다음과 같다.

$$R(\tau) = \sum_{t=0}^{N-1-\tau} \omega_M^{s(t) - s(t+\tau)}$$

여기서 $0 \leq \tau \leq N-1$ 이다. Sidel'nikov 는 M -진 수열을 다음과 같이 정의하였다 [1].

정의 1: p 가 소수이고 a 가 p^n 개의 원소를 갖는 유한체 F_{p^n} 의 원시원이라 하자. $M|(p^n-1)$ 이다. 이제 $k=0, 1, \dots, M-1$ 에 대해서 S_k 가 다음과 같이 정의되는 F_{p^n} 의 겹치지 않는 부분집합들이라 하자.

$$S_k = \{a^{Mi+k} - 1 \mid 0 \leq i \leq \frac{p^n-1}{M}\}$$

그러면 주기 p^n-1 인 Sidel'nikov 수열 $s(t)$ 는 다음과 같이 정의된다.

$$s(t) = \begin{cases} k, & \text{if } a^t \in S_k, 0 \leq k \leq M-1 \\ k_0, & \text{if } t = \frac{p^n-1}{2} \end{cases}$$

여기서 $0 \leq k_0 \leq M-1$ 인 임의의 정수이다. □

$k_0=0$ 인 M -진 Sidel'nikov 수열이 균형잡혀있다(balanced)는 것은 자명하다. 우리는 M -진 Sidel'nikov 수열을 지시 함수와 F_{p^n} 의 곱셈의 character를 사용해서 나타낼 수 있다.

정의 2: 지시 함수는 다음과 같이 정의된다.

$$I(x) = \begin{cases} 1, & \text{if } x = 0 \\ 0, & \text{if } x \neq 0 \end{cases}$$

□

정의 3: F_{p^n} 의 M 차의 곱셈 character는 다음과 같이 정의된다.

$$\Psi_M(a^t) = e^{j2\pi t/M}, \text{ if } a^t \in F_{p^n}^* \\ \Psi_M(0) = 0.$$

여기서 a 는 F_{p^n} 에서의 원시원이고 $M|(p^n-1)$ 이고 $0 \leq t \leq p^n-2$ 이다. □

그러면 M -진 Sidel'nikov 수열은 다음과 같이 나타낼 수 있다.

$$\omega_M^{s(t)} = \omega_M^{k_0} I(a^t + 1) + \Psi_M(a^t + 1) \quad (1)$$

뒤에서 Sidel'nikov 수열의 자기상관분포와 원분수(cyclotomic number) 사이의 관계가 유도된다.

정의 4: [3] a 가 F_{p^n} 에서의 원시원이라 하자. F_{p^n} 에서의 원분군(cyclotomic class) C_u , $0 \leq u \leq M-1$ 는 다음과 같이 정의된다.

$$C_u = \{a^{Ml+u} \mid 0 \leq l < \frac{p^n-1}{M}\}$$

여기서 주어진 u 와 v 에 대해서 원분수 $(u, v)_M = 1 + z \in C_v$ 를 만족하는 $z \in C_u$ 인 원소의 개수로 정의된다. □

다음 보조정리는 원분수들 사이의 기본적인 관계들을 보여준다.

보조정리 5: [3]

1) 임의의 정수 l_1, l_2 에 대해서

$$(i + Ml_1, j + Ml_2)_M = (i, j)_M$$

2) $(i, j)_M = (M-i, j-i)_M$

3) $(i, j)_M =$

$$\begin{cases} (j, i)_M, & \text{if } (p^n-1)/M \text{ is even} \\ (j + M/2, i + M/2), & \text{if } (p^n-1)/M \text{ is odd} \end{cases}$$

4) $\sum_{j=0}^{M-1} (i, j)_M = (p^n-1)/M - \Theta_i$, 여기서

$$\Theta_i = \begin{cases} 1, & \text{if } (p^n-1)/M \text{ is even and } i=0 \\ 1, & \text{if } (p^n-1)/M \text{ is odd and } i=M/2 \\ 0, & \text{otherwise} \end{cases}$$

5) $\sum_{i=0}^{M-1} (i, j)_M = (p^n-1)/M - \Theta_j$, 여기서

$$\Theta_j = \begin{cases} 1, & \text{if } j=0 \\ 0, & \text{otherwise} \end{cases}$$

III. Sidel'nikov 수열의 자기상관 특성

[4]로부터, 우리는 곱셈 character의 유용한 성질들을 얻을 수 있다.

성질 6: ^[4] $M|(p^n - 1)$ 라 하자. F_{p^n} 의 곱셈 character $\psi_M(x)$ 는 다음과 같은 성질을 갖는다.

- 1) $\sum_{x \in F_{p^n}} \psi_M(x) = 0$
- 2) $a \in F_{p^n}^*$ 일 때 $\overline{\psi_M(a)} = \psi_M^{-1}(a) = \psi_M(a^{-1})$
- 3) $a, b \in F_{p^n}$ 일 때 $\psi_M(a)\psi_M(b) = \psi_M(ab)$
- 4) $a \in F_{p^n}$ 이고 $b \in F_{p^n}^*$ 일 때 $\psi_M(a)\overline{\psi_M(b)} = \psi_M(a/b)$

여기서 $\overline{\psi}$ 는 ψ 의 켈레복소수를 의미한다. □

성질 6을 사용해서 M -진 Sidel'nikov 수열의 자기상관 함수는 다음과 같이 유도될 수 있다.

정리 7: ^[1] $s(t)$ 가 다음과 같이 주어지는 주기가 $N = p^n - 1$ 인 M -진 Sidel'nikov 수열이라 하자.

$$s(t) = \begin{cases} k, & \text{if } a^t \in S_k \\ k_0, & \text{if } t = (p^n - 1)/2. \end{cases}$$

그러면 $\tau \neq 0 \pmod{p^n - 1}$ 인 경우 $s(t)$ 의 자기상관 함수는 다음과 같이 주어진다.

$$R(\tau) = \omega_M^{k_0} \overline{\psi_M(1 - a^\tau)} + \omega_M^{-k_0} \psi_M(1 - a^{-\tau}) - \psi_M(a^{-\tau}) - 1$$

증명: Sidel'nikov에 의해 유사한 증명은 이미 제시되었지만 ^[1] 여기서는 본 정리 이후의 따름정리를 위해서 다시 자세히 증명하도록 하겠다.

(1)을 사용해서, $s(t)$ 의 자기상관함수인 $R(\tau)$ 는 다음과 같이 쓸 수 있다.

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{N-1} [(\omega_M^{k_0} I(a^t + 1) + \overline{\psi_M(a^t + 1)}) \\ &\quad \times (\omega_M^{-k_0} I(a^{t+\tau} + 1) \overline{\psi_M(a^{t+\tau} + 1)})] \\ &= \sum_{t=0}^{N-1} [I(a^t + 1)I(a^{t+\tau} + 1) \\ &\quad + \omega_M^{k_0} I(a^t + 1) \overline{\psi_M(a^{t+\tau} + 1)} \\ &\quad + \overline{\psi_M(a^t + 1)} \omega_M^{-k_0} I(a^{t+\tau} + 1) \\ &\quad + \psi_M(a^t + 1) \overline{\psi_M(a^{t+\tau} + 1)}] \end{aligned}$$

명백하게, $\tau \neq 0 \pmod{N}$ 일 때 $I(a^t + 1) \times I(a^{t+\tau} + 1) = 0$ 이고 다음이 성립한다.

$$\begin{aligned} R(\tau) &= \omega_M^{k_0} \overline{\psi_M(-a^\tau + 1)} + \omega_M^{-k_0} \psi_M(-a^{-\tau} + 1) \\ &\quad + \sum_{t=0}^{N-1} \psi_M(a^t + 1) \overline{\psi_M(a^{t+\tau} + 1)} \end{aligned}$$

성질 6을 사용하면 다음 식을 얻는다.

$$\begin{aligned} &\sum_{t=0}^{N-1} \psi_M(a^t + 1) \overline{\psi_M(a^{t+\tau} + 1)} \\ &= \sum_{t=0, t \neq (p^n - 1)/2}^{N-1} \psi_M\left(\frac{a^t + 1}{a^{t+\tau} + 1}\right) \end{aligned} \quad (2)$$

t 가 $(p^n - 1)/2 - \tau$ 를 제외하고 0부터 $N - 1$ 까지 변할 때, $(a^t + 1)/(a^{t+\tau} + 1)$ 은 집합 $F_{p^n} \setminus \{1, a^{-\tau}\}$ 의 모든 원소를 나타내게 된다. 그러면 (2)는 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned} &\sum_{t=0, t \neq (p^n - 1)/2}^{N-1} \psi_M\left(\frac{a^t + 1}{a^{t+\tau} + 1}\right) \\ &= -\psi_M(a^{-\tau}) - \psi_M(1) \end{aligned}$$

따라서 우리는 $\tau \neq 0$ 일 때 다음 식을 얻는다.

$$\begin{aligned} R(\tau) &= \omega_M^{k_0} \overline{\psi_M(1 - a^\tau)} + \omega_M^{-k_0} \psi_M(1 - a^{-\tau}) \\ &\quad - \psi_M(a^{-\tau}) - 1 \end{aligned} \quad \square$$

$F_{p^n} \setminus \{0, 1\}$ 에서 $y = a^t$ 라 하자. $\psi_M(-1) \psi_M(1/y) = \psi_M(1/(1-y)) \psi_M((y-1)/y)$ 로부터 우리는 정리 7을 좀 더 유용한 형태로 다음과 같이 바꿀 수 있다.

따름정리 8: M -진 Sidel'nikov 수열의 자기상관 함수는 다음과 같이 수정할 수 있다.

$\psi_M(-1) = 1$ 일 경우

$$\begin{aligned} R(y) &= -\left(\omega_M^{k_0} \psi_M\left(\frac{1}{1-y}\right) - 1\right) \\ &\quad \times \left(\omega_M^{-k_0} \psi_M\left(\frac{y-1}{y}\right) - 1\right) \end{aligned}$$

$\psi_M(-1) = -1$ 일 경우

$$\begin{aligned} R(y) &= \left(\omega_M^{k_0} \psi_M\left(\frac{1}{1-y}\right) + 1\right) \\ &\quad \times \left(\omega_M^{-k_0} \psi_M\left(\frac{y-1}{y}\right) + 1\right) - 2. \end{aligned}$$

$\psi_M(1/(1-y)) = \omega_M^u$ 와 $\psi_M((y-1)/y) = \omega_M^v$ 인 $y \in F_{p^n} \setminus \{0, 1\}$ 에 대해서 자기상관 함수 $R(y)$ 는 다음과 같이 쓸 수 있다.

$$R_{u,v} = -(\omega_M^{u+k_0} - 1)(\omega_M^{v-k_0} - 1), \text{ for } \Psi_M(-1) = 1 \quad (3)$$

$$R_{u,v} = (\omega_M^{u+k_0} + 1)(\omega_M^{v-k_0} + 1) - 2, \text{ for } \Psi_M(-1) = -1. \quad (4)$$

다음의 보조정리는 $\Psi_M(-1)$ 이 언제 1과 -1을 갖는지를 말해준다. 자세한 증명은 생략한다.

보조정리 9: $M|(p^n - 1)$ 라 하자. $p=2$ 일 때 $\Psi_M(-1) = \Psi_M(1) = 1$ 이다. 홀수인 소수 p 에 대해서 다음이 성립한다.

$$\Psi_M(-1) = \begin{cases} +1, & \text{if } (p^n - 1)/M \text{ is even} \\ -1, & \text{if } (p^n - 1)/M \text{ is odd.} \end{cases} \quad \square$$

IV. Sidel'nikov 수열의 자기상관 분포

이 장에서 우리는 따름정리 8에서 주어진 M -진 Sidel'nikov 수열의 자기상관 함수의 값들을 유도한 후에 차수가 M 인 원분수의 형태로 각각의 값들의 발생회수를 나타낼 것이다. 다음의 보조정리는 M -진 Sidel'nikov 수열의 위상이 다를 때의 가능한 서로 다른 자기상관 값들의 개수를 보여준다. 여기서 '가능한'이라는 말은 자기상관 값들 중 어떤 것들은 M 과 수열의 주기에 따라서 에 따라서 발생하지 않을 수도 있다는 사실을 의미한다.

보조정리 10: M -진 Sidel'nikov 수열의 위상이 다를 때의 서로 다른 자기상관 값들의 개수는 다음 값보다 작거나 같다.

$$\frac{M(M-1)}{2} + 1.$$

증명: $k_0 \neq 0$ 인 서로 다른 $R_{u,v}$ 의 개수는 $k_0 = 0$ 인 $R_{u,v}$ 의 개수와 같다는 것은 분명하다. 그래서 우리는 $k_0 = 0$ 인 경우만을 증명할 것이다. $u=0$ 이거나 $v=0$ (또는 $u=M/2$ 이거나 $v=M/2$)일 때 $R_{u,v} = 0$ (또는 -2)인 것은 쉽게 알 수 있다. $R_{u,v} = R_{v,u}$ 이기 때문에 위에서와 같은 위상이 다를 때의 서로 다른 자기상관 값들의 개수를 구하는 것은 어렵지 않다. \square

위상이 다를 때의 자기상관 값들 중 어떤 것들이

발생하지 않을 수 있다는 것은 분명하다. 특히 수열의 주기에 비해서 알파벳 크기 M 이 큰 경우에는 더욱 그렇다.

따름정리 8은 자기상관 분포가 아래와 같이 정의되는 집합 $S_{u,v}$ 의 cardinality인 $A_{u,v}$ 에만 의존한다는 것을 말해준다.

$$S_{u,v} = \{y \in F_p \setminus \{0, 1\} \mid \Psi_M(1/(1-y)) = \omega_M^u, \Psi_M(y-1/y) = \omega_M^v\}.$$

여기서 $u, v \in \{0, 1, 2, \dots, M-1\}$ 이다.

그러면 $A_{u,v}$ 는 다음 정리에서처럼 차수가 M 인 원분수로 나타낼 수가 있다.

정리 11: $A_{u,v}$ 는 다음과 같은 관계가 있다.

$$A_{u,v} = (u+v, v)_M.$$

증명:

경우 1) $\Psi_M(-1) = 1$ 일 때.

$\Psi_M(1/(1-y)) = \omega_M^u$, $\Psi_M((y-1)/y) = \omega_M^v$ 로부터 $\Psi_M(1/(1-y))\Psi_M((y-1)/y) = \Psi_M(1/y) = \omega_M^{u+v}$ 를 얻을 수 있다. 다시 말해 $1-y \in C_{-u}$ 이고 $y \in C_{-u-v}$ 이다. $-y$ 와 y 가 같은 원분군에 있기 때문에 보조정리 5의 2)를 적용하면 다음을 얻는다.

$$A_{u,v} = (-u-v, -u)_M = (u+v, v)_M.$$

경우 2) $\Psi_M(-1) = -1$ 일 때.

$\Psi_M(1/(1-y))\Psi_M((y-1)/y) = \Psi_M(-1/y) = \omega_M^{u+v}$ 이다. 그래서 $1-y \in C_{-u}$ 와 $-y \in C_{-u-v}$ 를 얻는다. 그래서 마찬가지로 관계식 $A_{u,v} = (-u-v, -u)_M = (u+v, v)_M$ 를 얻었다. \square

이제 Sidel'nikov 수열의 자기 상관 분포를 다음 정리에서처럼 구할 수 있다.

정리 12: $N(R_{u,v})$ 가 $R(y) = R_{u,v}$ 를 만족하는 $y \in F_p \setminus \{0, 1\}$ 의 개수라 하자. 그러면 주기가 $p^n - 1$ 인 M -진 Sidel'nikov 수열의 위상이 다를 때의 자기상관 분포는 다음과 같이 주어진다.

만일 $\Psi_M(-1) = 1$ 이면,

$$1) \quad N(0) = \sum_{i=0}^{M-1} ((i, i+k_0)_M + (i, k_0)_M) + (0, k_0)_M$$

- 2) $N(R_{k,k}) = (2k, k+k_0)_M, 1 \leq k \leq M-1$
- 3) $N(R_{u,v}) = (u+v, v+k_0)_M$
 $+ (u+v, u+k_0)_M, 1 \leq u < v \leq M-1$

만일 $\psi_M(-1) = -1$ 이면,

- 1) $N(-2) = \sum_{i=0, i \neq M/2}^{M-1} ((M/2+i, i+k_0)_M$
 $+ (M/2+i, M/2+k_0)_M) + (0, M/2+k_0)_M$
- 2) $N(R_{k,k}) = (2k, k+k_0)_M, 0 \leq k \leq M-1$ 이고 $k \neq M/2$
- 3) $N(R_{u,v}) = (u+v, v+k_0)_M$
 $+ (u+v, u+k_0)_M$
 $0 \leq u < v \leq M-1, u \neq M/2, \text{ 그리고 } v \neq M/2.$

증명: 만일 $\psi_M(-1) = 1$ 인 경우 다음 식이 성립한다.

$$R_{u,v} = -(\omega^{u+k_0} - 1)(\omega^{v-k_0} - 1).$$

그래서 다음 식을 얻는다.

$$N(0) = \sum_{u=0}^{M-1} A_{u, k_0} + \sum_{v=0}^{M-1} A_{k_0, v} - A_{-k_0, k_0}$$

$$= \sum_{i=1}^{M-1} ((i, i+k_0)_M + (i, k_0)_M) + (0, k_0)_M.$$

마찬가지로 다음의 두 개의 식을 얻을 수 있다.

$$N(R_{k,k}) = A_{k-k_0, k+k_0} = (2k, k+k_0)_M.$$

그리고

$$N(R_{u,v}) = A_{u-k_0, v+k_0} + A_{v-k_0, u+k_0}$$

$$= (u+v, v+k_0)_M + (u+v, u+k_0)_M.$$

$\psi_M(-1) = -1$ 인 경우의 증명도 비슷한 방식으로 할 수 있다. □

이제 우리는 M -진 Sidel'nikov 수열의 자기상관 값들의 최대 크기의 상한을 다음과 같이 쉽게 유도할 수 있다.

정리 13: M -진 Sidel'nikov 수열의 위상이 다를 때의 자기상관 값들의 최대 크기의 상한은 다음과 같이 주어진다.

만일 $\psi_M(-1) = 1$ 라면,

$$\max_{0 < \tau \leq p^n - 2} |R(\tau)|$$

$$\leq \begin{cases} 4, & \text{if } M \text{ is even} \\ 4 \cos^2(\pi/2M), & \text{if } M \text{ is odd.} \end{cases}$$

그리고 만일 $\psi_M(-1) = -1$ 라면,

$$\max_{0 < \tau \leq p^n - 2} |R(\tau)|$$

$$\leq \begin{cases} 2\sqrt{2}, & \text{if } M \equiv 0 \pmod{4} \\ 2\sqrt{\cos^2(\pi/M) + 1}, & \text{if } M \equiv 2 \pmod{4}. \end{cases}$$

증명: $R_{u,v}$ 의 최대 크기의 상한이 k_0 와 관계없다는 것은 자명하다. 그러므로 $k_0 = 0$ 인 경우에 대해서만 증명한다.

경우 1) 만일 $\psi_M(-1) = 1$ 라면, (3)로부터 M 이 짝수인 경우 $(u, v) = (\frac{M}{2}, \frac{M}{2})$ 일 때, 혹은 M 이 홀수인 경우 $(u, v) = (\frac{M+1}{2}, \frac{M+1}{2})$ 일 때, 자기상관 값이 최대 크기라는 것은 쉽게 보일 수 있다. 그러므로 (5)를 쉽게 유도할 수 있다.

경우 2) 만일 $\psi_M(-1) = -1$ 라면, (4)로부터, 자기상관함수는 다음과 같다.

$$R_{u,v} = 4 \cos\left(\frac{\pi u}{M}\right) \cos\left(\frac{\pi v}{M}\right)$$

$$\times \exp\left[j\left(\frac{\pi}{M}(u+v)\right)\right] - 2.$$

삼각함수의 변환을 이용하면, 다음과 같다.

$$|R_{u,v}|^2 = 4 \sin\left(\frac{2\pi u}{M}\right) \sin\left(\frac{2\pi v}{M}\right) + 4.$$

자기상관 값의 최대 크기는 $M \equiv 0 \pmod{4}$ 인 경우일 때 $(u, v) = (\frac{M}{4}, \frac{M}{4})$ or $(\frac{3M}{4}, \frac{3M}{4})$ 에서 구할 수 있다. 그리고 $M \equiv 2 \pmod{4}$ 인 경우에는, (u, v) 가 $(\frac{M+2}{4}, \frac{M+2}{4})$ 이거나 $(\frac{3M+2}{4}, \frac{3M+2}{4})$ 에서 자기상관 값이 최대이다. 그러므로 (6)를 쉽게 유도할 수 있다. □

V. 예 제

F_p^n 에서의 차수가 2, 3, 4, 6, 8인 원분수는 [3]에서 구하였다. 앞의 결과와 이미 알려진 원분수 $(u, v)_M$ 를 사용해서, 2진, 3진, 4진, 6진, 8진 Sidel'nikov 수열의 자기상관 분포를 구할 수 있다.

여기에서는, 3진 Sidel'nikov 수열의 자기상관 분포를 계산한다. 따름정리 8을 사용하면, 다음의 따름정리를 얻을 수 있다.

따름정리 14: 주기가 $p^n - 1$ 이고 $k_0 = 0$ 인 3진

($M=3$) Sidel'nikov 수열의 자기상관 분포는 다음과 같다.

$$R_{u,v} = \begin{cases} p^n - 1, & \text{once} \\ 0, & \frac{5p^n - 16 - c}{9} \text{ times} \\ -3, & \frac{2p^n - 4 - c}{9} \text{ times} \\ 3\omega_3, & \frac{p^n + 1 + c}{9} \text{ times} \\ 3\omega_3^2, & \frac{p^n + 1 + c}{9} \text{ times} \end{cases}$$

여기서 $4p^n = c^2 + 27d^2$, $c \equiv 1 \pmod{3}$ 이고, ω_3 는 3차 복소단위원이다. □

다음은 주기가 $7^3 - 1$ 이고 $k_0 = 0$ 인 3진 Sidel'nikov 수열의 자기상관 분포에 대한 예제이다.

예제 15: $p=7$ 과 $n=3$ 라 하자. $4p^n = c^2 + 27d^2$ 과 $c \equiv 1 \pmod{3}$ 로부터, $c = -20$ 와 $d = \pm 6$ 라는 값을 구할 수 있다. 따름정리 14로부터, 다음을 얻는다.

$$R(\tau) = \begin{cases} 342, & \text{once} \\ 0, & 191 \text{ times} \\ -3, & 78 \text{ times} \\ 3\omega_3, & 36 \text{ times} \\ 3\omega_3^2, & 36 \text{ times.} \end{cases}$$

□

참 고 문 헌

- [1] V. M. Sidel'nikov, "Some k -valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 1, pp. 12-16, 1969.
- [2] A. Lempel, M. Cohn, and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 38-42, Jan. 1977.
- [3] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL: Markham Publishing Company, 1967.
- [4] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*, Reading, MA: Addison-Wesley, 1983.

김 영 식 (Young-Sik Kim)

준회원



호, 디지털통신

2001년 2월 서울대학교 전기공학부(공학사)
 2003년 2월 서울대학교 전기컴퓨터공학부(석사)
 2003년 3월~현재 서울대학교 전기컴퓨터공학부 박사과정
 <관심분야> 시퀀스, 오류정정부

정 정 수 (Jung-Soo Chung)

준회원



2003년 2월 서울대학교 전기컴퓨터공학부(공학사)
 2003년 3월~현재 서울대학교 전기컴퓨터공학부 석박사통합과정
 <관심분야> 시퀀스, 오류정정부
 호, 디지털 통신

노 종 선 (Jong-Seon No)

중신회원



1981년 2월 서울대학교 전자공학과(공학사)
 1981년 2월 서울대학교 전자공학과(공학사)
 1984년 2월 서울대학교 대학원 전자공학과(석사)
 1988년 5월 University of Southern California, 전기공학과(공학박사)
 1988년 2월~1990년 7월 Hughes Network Systems, Senior MTS
 1990년 9월~1999년 7월 건국대학교 전자공학과 부교수
 1999년 8월~현재 서울대학교 전기컴퓨터공학부 교수
 <관심분야> 시퀀스, 시공간부호, LDPC 부호, OFDM, 이동통신, 암호학

정 하 봉 (Habong Chung)

중신회원



학과(공학박사)

1981년 2월 서울대학교 전자공학과 졸업(공학학사)
 1985년 미국 University of Southern California, 전기공학과(공학석사)
 1988년 미국 University of Southern California, 전기공

1988년~1991년 미국 뉴욕주립대 전기공학과 조교수

1991년~현재 홍익대학교 전자전기공학부 교수

<관심분야> 부호 이론, 조합수학, 시퀀스 설계

김 경 아 (Kyung-ah Kim)

정회원



1989년 2월 이화여자대학교 전
자계산학과(학사)

1991년 2월 이화여자대학교 대
학원 전자계산학과(석사)

2004년 8월 서울대학교 공과대
학 컴퓨터공학부(공학박사)

1991년~현재 KT 통신망운용

연구소, 마케팅 연구소, 책임연구원

<관심분야> Mobile IP, Handover, Wireless Access
Network, Ad hoc Routing